МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учебно-методическое объединение по естественнонаучному образованию

УТВЕРЖДАЮ
Первый заместитель Министра образования Республики Беларусь
_____ В.А.Богуш
«20» 05 2015г.
Регистрационный № ТД-G.513 /тип.

Алгебра и теория чисел

Типовая учебная программа по учебной дисциплине

для направления специальности

1- 31 03 07 - 01 Прикладная информатика
(программное обеспечение компьютерных систем)

СОГЛАСОВАНО
Председатель
Учебно-методического объединения
по естественнонаучному
образованию
_____ П. Толстик
«20» 05 2015 г.

СОГЛАСОВАНО
Начальник Управления высшего образования Министерства образования Республики Беларусь
_____ С.И. Романюк
«20» 05 2015 г.

СОГЛАСОВАНО
Проректор по научно-методической работе Государственного учреждения образования «Республиканский институт высшей школы»
_____ И.В. Титович
«05» 05 2015 г.

Эксперт-нормоконтролер
_____ А.А. Денисевич
«27» 04 2015 г.

Минск 2015

СОСТАВИТЕЛИ:
Г.П. Размыслович, доцент кафедры высшей математики Белорусского государственного университета, кандидат физико-математических наук, доцент;
А.В. Филипцов, доцент кафедры высшей математики Белорусского государственного университета, кандидат физико-математических наук, доцент;
В.М. Ширяев, доцент кафедры высшей математики Белорусского государственного университета, кандидат физико-математических наук, доцент

РЕЦЕНЗЕНТЫ:
Кафедра высшей математики Учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»;
М.П.Дымков, заведующий кафедрой высшей математики Учреждения образования «Белорусский государственный экономический университет», доктор физико-математических наук, профессор

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ В КАЧЕСТВЕ ТИПОВОЙ
Кафедрой высшей математики Белорусского государственного университета (протокол № 12 от 17 апреля 2014г.);

Научно-методическим советом Белорусского государственного университета (протокол № 5 от 15 мая 2014г.);

Научно-методическим советом по прикладной математике и информатике учебно-методического объединения по естественнонаучному образованию (протокол № 7 от 22 апреля 2014г.).

Ответственный за редакцию: Г.П.Размыслович
Ответственный за выпуск: А.В.Филипцов

Пояснительная записка

Типовая учебная программа по учебной дисциплине «Алгебра и теория чисел» разработана в соответствии с типовым учебным планом и образовательным стандартом первой ступени высшего образования для направления специальности: 1- 31 03 07 - 01 «Прикладная информатика (программное обеспечение компьютерных систем)»

Учебная дисциплина «Алгебра и теория чисел» знакомит студентов с основными понятиями высшей алгебры и теории чисел.

Базой для изучения данной дисциплины является дисциплина «Алгебра», изучаемая в средней школе.

«Алгебра и теория чисел» является базовой математической учебной дисциплиной и непосредственно связана с основными дисциплинами аналитического цикла, такими как «Аналитическая геометрия» и «Математический анализ» государственного компонента. Методы, излагаемые в учебной дисциплине «Алгебра и теория чисел», используются при изучении учебных дисциплин «Дифференциальные уравнения», «Теория вероятностей и математическая статистика», «Методы вычислений», «Криптографические методы» государственного компонента.

Основными целями преподавания учебной дисциплины «Алгебры и теории чисел» являются:

– во-первых, дать глубокие знания по одному из основных разделов курса высшей математики, имеющего тесную связь с многочисленными прикладными проблемами и богатые приложения;

– во-вторых, создать фундамент, необходимый для усвоения материала перечисленных выше дисциплин;

– в-третьих, сформировать одну из основных частей банка знаний специалистов университетского уровня в избранной области деятельности.

Основные задачи, решаемые при изучении учебной дисциплины «Алгебра и теория чисел»:

- изучение основ теории чисел;
- изучение основ линейной алгебры.

При изложении курса важно показать возможности использования аппарата алгебры и теории чисел при решении как чисто теоретических, так и прикладных задач, возникающих в различных областях науки, техники, экономики и др. Целесообразно выделить моменты построения алгоритмов полученных результатов с целью их реализации при помощи средств вычислительной техники.

В результате изучения дисциплины студент должен

знать:

- основы теории чисел и ее применение в информатике;
- основные понятия высшей алгебры;
- основы линейной алгебры;

уметь:

– находить решения показательных, степенных сравнений с использованием таблицы индексов и решения систем сравнений;

– применять аппарат алгебры при решении задач специальности;

– решать основные задачи теории векторных, евклидовых пространств.

владеть:

– навыками решения основных задач теории чисел и линейной алгебры;

– методами алгебры и теории чисел при решении задач специальности.

Типовая учебная программа рассчитана на 208 учебных часа, в том числе 136 аудиторных часов, примерное распределение которых по видам занятий включает лекции – 68 часов, практические занятия – 68 часов.

Рекомендуемая форма текущей аттестации – экзамен, зачеты.

В соответствии с требованиями образовательного стандарта по специальности 1-31 03 07 «Прикладная информатика (по направлениям)» специалист должен владеть следующими академическими компетенциями (АК) и профессиональными компетенциями (ПК):

АК-1. Уметь применять базовые научно-теоретические знания для решения теоретических и практических задач.

АК-2. Владеть системным и сравнительным анализом.

АК-3. Владеть исследовательскими навыками.

АК-4. Уметь работать самостоятельно.

АК-5. Быть способным порождать новые идеи (обладать креативностью).

АК-6. Владеть междисциплинарным подходом при решении проблем.

ПК-7. Применять профессиональные знания и навыки для проведения научных исследований в области прикладной информатики.

ПК-10. Формулировать выводы и рекомендации по применению результатов научно-исследовательской работы.

ПК-29. Взаимодействовать со специалистами смежных профилей.

Примерный тематический план

№	Название раздела, темы	Количество аудиторных часов		
		Всего	В том числе	
			Лекции	**Практические занятия**
	Введение.	1	1	
	Раздел 1. Теория чисел			
1.	Делимость чисел	7	3	4
2.	Простые числа и составные числа	4	2	2
3.	Числовые сравнения	8	4	4
4.	Сравнения с одним неизвестным	8	4	4
5.	Системы сравнений первой степени	8	4	4
6.	Приложения теории чисел	4	2	2
	Раздел 2. Алгебра.			
7.	Алгебраическая операция. Группа, кольцо, поле	8	4	4
8.	Комплексные числа	8	4	4
9.	Многочлены	8	4	4
10.	Матрицы и определители	12	6	6

11.	Векторные пространства	12	6	6
12.	Системы уравнений	8	4	4
13.	Линейные отображения	12	6	6
14.	Квадратичные формы	8	4	4
15.	Евклидово пространство	8	4	4
16.	Изометрические и симметрические преобразования	8	4	4
17.	Элементы линейного программирования	4	2	2
	Всего	**136**	**68**	**68**

Содержание учебного материала

Введение

Предмет дисциплины «Алгебра и теория чисел». Исторические сведения о развитии этого раздела математики. Роль и место теории чисел и алгебры в системе математического образования.

Раздел 1. Теория чисел

1. Делимость чисел

Свойства отношения делимости целых чисел. Деление с остатком. Наибольший общий делитель и наименьшее общее кратное. Алгоритм Евклида.

2. Простые числа и составные числа

Простые числа и их свойства. Взаимно простые числа, критерий взаимной простоты. Свойства взаимной простоты. Разложение числа в произведение элементарных делителей.

3. Числовые сравнения

Сравнения целых чисел по данному модулю и их свойства. Кольцо вычетов по данному модулю. Приведенная группа вычетов. Функция Эйлера, свойства. Теорема Эйлера, малая теорема Ферма.

4. Сравнения с одним неизвестным

Решение сравнений первой степени. Существование первообразного элемента по простому модулю, по примарному модулю и по двойному примарному модулю. Свойства индексов. Решение показательных и степенных сравнений.

5. Системы сравнений первой степени

Решение систем линейных уравнений над кольцом целых чисел. Китайская теорема об остатках.

6. Приложения теории чисел

Разделение секрета и пороговая схема. Протокол Диффи-Хелмана. RSA-криптосистема и система цифровой подписи на её основе.

Раздел 2. Алгебра

7. Алгебраическая операция. Группа, кольцо, поле

Бинарное отношение. Отношения эквивалентности и порядка, классы эквивалентности. Алгебраическая операция. Группа, кольцо, поле и их простейшие свойства.

8. Комплексные числа

Построение поля комплексных чисел. Алгебраическая, тригонометрическая и экспоненциальная формы комплексных чисел. Возведение в степень и извлечение корня n-ой степени из комплексного числа. Корни из единицы.

9. Многочлены

Кольцо многочленов над полем. Деление с остатком. Алгоритм Евклида. Схема Горнера. Корни многочлена. Разложение многочленов на неприводимые многочлены. Интерполяция.

10. Матрицы и определители

Матричная алгебра. Определители. Теорема Лапласа. Обратная матрица. Системы линейных уравнений. Правило Крамера. Метод Гаусса. Матричные уравнения.

11. Векторные пространства

Векторное (линейное) пространство. Линейная зависимость и независимость систем векторов. Базис и размерность. Подпространства. Линейные оболочки. Сумма и пересечение подпространств. Ранг системы векторов. Ранг матрицы и теорема о ранге матрицы и следствия из нее.

12.Системы уравнений

Критерий совместности систем линейных уравнений над полем. Подпространство решений однородной системы уравнений. Связь между решениями неоднородной системы уравнений и соответствующей однородной системы уравнений.

13. Линейные отображения

Матрица линейного отображения. Подобные матрицы. Ядро и образ линейного отображения. Невырожденное линейное преобразование. Собственные векторы и собственные значения. Характеристическая матрица и характеристический многочлен. Аннулирующий многочлен, минимальный многочлен матрицы. Теорема Гамильтона-Кели. Матрица Жордана.

14. Квадратичные формы

Каноническая квадратичная форма. Метод выделения полных квадратов приведения квадратичной формы к каноническому виду. Критерии эквивалентности квадратичных форм над полем R и над полем C. Знакоопределённые действительные квадратичные формы.

15. Евклидово пространство

Свойства скалярного произведения в евклидовых пространствах. Длина вектора. Матрица Грама и матрица скалярного произведения. Процесс ортогонализации Грама-Шмидта.

16. Изометрические и симметрические преобразования

Изометрический оператор, связь с ортогональными и унитарными матрицами. Самосопряжённый оператор. Существование ортонормированного базиса из собственных векторов самосопряженного оператора. Приведение вещественной квадратичной формы к каноническому виду при помощи ортогонального преобразования переменных.

17. Элементы линейного программирования

Представление выпуклого многогранного множества. Общее решение системы линейных неравенств. Задача линейного программирования. Опорные планы.

Информационно-методическая часть

Литература

Основная

1. Айерленд К., Роузен М. Классическое введение в теорию чисел. М., "Мир", 1987. 415с.

2. Арнольд И.В. Теория чисел. М., 1939. 288с.

3. Беняш-Кривец В.В., Мельников О.В. Лекции по алгебре. Группы, кольца, поля. Мн.:БГУ, 2009г., 115с.

4. Биркгоф Г., Барти Т. Современная прикладная алгебра. М., 2005г., 400с.

5. Бурдун А.А., Мурашко Е.А., Толкачев М.М., Феденко А.С. Сборник задач по алгебре и аналитической геометрии. – Мн., "Университетское", 1989, 222с

6. Виноградов И.М. Теория чисел. М., Наука, 1981. с.

7. Заславский Ю.Л. Сборник задач по линейному программированию. М. 1969г. 256с.

8. Ильин В.А., Позняк Э.Г. Линейная алгебра. – М: "Наука", 1981г., 294с

9. Милованов М.В., Тышкевич Р.И., Феденко А.С. Алгебра и аналитическая геометрия. I. – Мн., "Выш. школа", 2001г., 400с.

10. Милованов М.В., Тышкевич Р.И., Феденко А.С. Линейная алгебра и аналитическая геометрия. II. – Мн., "Выш. школа", 1984г., 302с.

11. Нестеренко Ю.В. Теория чисел. М., "Академия", 2008. 272с.

12. Размыслович Г.П., Феденя М.М., Ширяев В.М. Геометрия и алгебра. – Мн., "Университетское", 1987г., 350с.

13. Размыслович Г.П., Феденя М.М., Ширяев В.М. Сборник задач по геометрии и алгебре. – Мн., "Университетское", 1999г., 384с

14. Харин Ю.С. Математические и компьютерные способы криптографии. Мн., 2003г., 391с.

15. Ширяев В.М. Прикладная алгебра. Теория чисел. Сборник задач. Мн.: БГУ, 2009г., 152с.

16. Шнеперман Л.Б. Сборник задач по алгебре и теории чисел. Мн: "Выш. школа", 1982, 223с.

17. Шнеперман Л.Б. Курс алгебры и теории чисел в задачах и упражнениях. Т1., Мн: "Выш. школа", 1986, 272с.

Дополнительная

1. Винберг Э.Б. Курс алгебры. М. 1999г., 528с.
2. Воеводин В.В. Линейная алгебра. – М., "Наука", 1990, 400с.
3. Курош А.Г. Курс высшей алгебры. – М., "Наука", 1975, 431с.
4. Кострикин А.И., Манин Ю.И. Линейная алгебра и геометрия. М.: "Наука", 1986г., 304с.
5. Ланкастер П. Теория матриц. М. 1978г., 280с
6. Нечаев В.И. Элементы криптографии, основы защиты информации. М. 1999г., 109с.
7. Проскуряков И.В. Сборник задач по линейной алгебре. М.: "Наука", 1978г., 384с.
8. Фаддеев Д.Н., Соминский И.С. Сборник задач по высшей алгебре. – М.: "Наука", 1977, 188с.

Диагностика компетенций студентов

Условия для самостоятельной работы студентов, в частности, для развития навыков самоконтроля, способствующих интенсификации учебного процесса, обеспечиваются наличием и полной доступностью электронных (и бумажных) вариантов курсов лекций, учебно-методических пособий и сборников задач по основным разделам дисциплины.

Текущий контроль усвоения знаний рекомендуется осуществлять в виде собеседований и коллоквиумов по теоретическому материалу и в виде письменных контрольных работ и отчетов по домашним заданиям по практическому материалу.

Рекомендуемая форма текущей аттестации – экзамен, зачеты.